

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Victoria M. BELLOTTI et al.

Group Art Unit: 2145

Application No.: 09/683,532

Examiner: A. CHOUDHURY

Filed: January 16, 2002

Docket No.: 110143

For: SYSTEMS AND METHODS FOR INTEGRATING ELECTRONIC MAIL AND
DISTRIBUTED NETWORKS INTO A WORKFLOW SYSTEM

PRE-APPEAL BRIEF REQUEST FOR REVIEW


Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This request is being filed with a Notice of Appeal and Petition for Extension of Time. Review of the November 19, 2007 Final Rejection is requested for the reasons set forth in the attached five or fewer sheets. Applicants note that a response to the November 19 Final Rejection was filed within two-months of the mail date of the Final Rejection. As such, the period for reply expired on the mail date of the March 26, 2008 Advisory Action. Only a one-month extension of time is required.

Should any questions arise regarding this submission, or the Review Panel believe that anything further would be desirable in order to place this application in even better condition for allowance, the Review Panel is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,


James A. Oliff
Registration No. 27,075

James E. Golladay, II
Registration No. 58,182

JAO:JEG/clf

Date: April 18, 2008

REMARKS

Claims 1-22 and 25 are pending in this application. The Office Action rejects claims 1-22 and 25 under 35 U.S.C. §103(a) over "Implementation of a Workflow-based Web Application with an Electronic Signature Mechanism," by Kim et al. (hereinafter "Kim") in view of U.S. Patent Application Publication No. 2002/0133495 to Rienhoff Jr. et al. (hereinafter "Rienhoff"). This rejection is respectfully traversed.

With regard to claims 1 and 10, the Office Action concedes that Kim does not disclose that the recipient of the email message does not have access to the workflow system prior to receipt of the e-mail message. The Office Action relies on Rienhoff to remedy the shortfall. The Office Action alleges that Rienhoff teaches how a user gains access to a secured area of a site after clicking on a link that can be received through an e-mail. The Office Action summarily concludes that it would have been obvious to one of ordinary skill in the art to combine Rienhoff with Kim in order to "restrict access to secure content". These assertions are incorrect for at least the following reasons.

The conclusory statement that one of ordinary skill in the art would have been motivated to combine the alleged teachings of Rienhoff with the Kim system in order to restrict access to secure content fails to recognize that Kim already restricts access to secure content. Thus, one of ordinary skill in the art would not have been motivated to combine the alleged teachings of Rienhoff with Kim as asserted by the Office Action.

The Examiner responds that, in the Examiner's opinion, Kim's design does not let users have access to the workflow system (secured areas) prior to the receipt of the e-mail embedded with a link. This response apparently concedes the premise of Applicants' argument that one of ordinary skill in the art would not have been motivated to combine the alleged teachings of Rienhoff with Kim because Kim already "restricts access to secure content." Applicants maintain that a *prima facie* case of obviousness has not been established

with respect to how any object lacking in Kim would be achieved with a reasonable expectation of success based on the alleged teachings of Rienhoff.

Moreover, contrary to the assertion of the Office Action and the Examiner's response in the March 26, 2008 Advisory Action, Rienhoff does not teach, nor can it reasonably be considered to have suggested, the relied-upon features. For example, the allegedly corresponding e-mail in Rienhoff may direct a user to a secure area of a website, but "access" to the secured area of the website is only gained by logging on with, for example, the log-in name and password established in step 750 (see paragraphs [0106] and [0113] of Rienhoff). Thus, the allegedly corresponding e-mail in Rienhoff does not provide a recipient who does not have access to the workflow system with an access to an associated process of the workflow system, as recited, for example, in claim 1.

The Office Action asserts that Rienhoff allegedly does not require a login when accessing the secured area. The Office Action asserts that a secondary login setup is available, but is optional in Rienhoff. The Office Action refers to paragraph [0112] of Rienhoff in support of this assertion. However, the Office Action misinterprets the disclosure of Rienhoff with respect to these features.

Rienhoff states that "in some embodiments, the user may be given, or requested to establish, an additional login name and/or password to permit them access to the secured area" (emphasis added). The Office Action interprets this to mean that access to a secured area of a site does not require a login as asserted, but is, rather, accessible via a link. However, paragraph [0113] clarifies that, in step 780, the user logs into the secured area of the website. The user may login with the login name and password established in step 750. Alternatively, if the user established a login name and password in step 776, the user may login with the log in name and password established in step 776. Thus, the language of paragraph [0112] clearly means that what is "optional" is whether an additional login name

and/or password will be established. Step 780, actually logging in to the secure area, with some login name and password, is not optional. Rienhoff teaches that a user will login to establish access to the secured area of the website either by the login name and password established in step 750, or the login name and password established in step 776.

As such, the allegedly corresponding e-mail in Rienhoff does not provide a recipient who does not have to access to the workflow system with an access to an associated process of the workflow system, as recited, for example, in claim 1.

The Advisory Action maintains, in part, that Rienhoff allows access to a secured area of the site without a log in. However, as indicated above, Rienhoff requires one of two potential logins to gain access to the secured area of the site. Applicants maintain that Step 780 in Rienhoff, actually logging in to the secure area, with some login name and password, is not optional.

In this regard, the Office Action fails to consider all of the features of the claim in maintaining the above assertion. For example, claim 1 recites, among other features, creating an email message to a recipient by a user, the recipient who does not have access to the workflow system; embedding a link to a determined network address in the email message to the recipient; associating a process of the workflow system with the determined network address; and sending the email message having the link to the determined network address to the recipient, wherein the link provides the recipient with an access to the associated process of the workflow system. The combination of Kim and Rienhoff would not have reasonably suggested this combination of features, or those recited in claims 8, 9, 19, 20 or 25.

With regard to claims 4, 5, 13 and 14, the Office Action asserts that Kim teaches randomly or pseudo-randomly generating the network address. This assertion is incorrect. Kim does not address the relevant network addresses being generated. The Office Action apparently relies on a section in Kim that deals with generating an electronic signature key as

teaching the generation of network address. However, the generating of the electronic signature key described in Kim does not correspond to generating a network address.

Regarding claims 8, 9, 19 and 20, the Office Action concedes that Kim does not teach embedding multiple links within a single e-mail. The Office Action relies on Official Notice that is well known in the art that a plurality of links can be embedded in an e-mail for the purpose of sending multiple links without using multiple messages. However, such a modification of Kim would impermissibly alter Kim's method of operation and render it unsuitable for its intended purpose. Specifically, Kim teaches sending decision makers individual e-mails, specific to certain documents, with individual random keys. As such, careful control of the sequence of approval is achieved (see section 3.3 of Kim). Incorporating multiple links, *e.g.* to various stages of the workflow process of Kim, with all of the corresponding random keys required by Kim, would defeat this purpose, rendering the invention of Kim unsuitable for its intended purpose.

The Advisory Action maintains the response that "no alteration in methods of operation is required for embedding multiple links versus one link, within an e-mail." This analysis does not meaningfully address Applicants' argument that Kim's method of operation involves sending decision makers individual e-mails, specific to certain documents, with individual random keys. Including multiple links within a single e-mail would clearly alter this method of operation. Additionally, the Examiner does not address the separate argument that such a modification would render Kim unsatisfactory for its intended purpose (see MPEP §2143.01 (V)). Applicants maintain that the asserted modification of Kim, to include multiple links within a single e-mail, would not have been obvious for at least these reasons.

Regarding claim 25, the Office Action asserts that Kim teaches excluding generating network addresses that have been embedded in previous e-mail messages created by the system that have not yet been accessed. The Advisory Action relies on page 2, second

column, lines 25-40 of Kim as teaching such a feature. The Advisory Action asserts that because Kim teaches that data within an e-mail, including the URL, can be encrypted to prevent it from being exposed, this means that the URL within each e-mail is "unique." This assertion is incorrect and does not address the relevant features of claim 25.

For example, the fact that information may be encrypted for transmission, and decrypted for use, does not mean that URLs within each e-mail are unique. For example, if the same URL were sent to several users via encryption, even though each message might contain different encrypted data, the URL may be the same.

Moreover, this does not correspond to excluding generated network addresses that have previously been embedded in any previous e-mail messages created by the system that have not yet been accessed. The features of claim 25 allow for network addresses that have been accessed to be used again. There is no teaching or suggestion in the applied references of excluding generated network addresses that have previously been embedded in any previous e-mail messages created by the system that have not yet been accessed.

In view of the foregoing, Applicants respectfully request that the Review Panel review the substance of the November 19, 2007 rejection in light of the above remarks. Applicants believe, upon such review, the Review Panel will determine that at least the rejections of claims 1, 4, 5, 8-10, 13, 14, 19-21 and 25 and the claims depending therefrom, are unreasonable. In this regard, favorable reconsideration and prompt allowance of claims 1-22 and 25 are earnestly solicited.